UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

IN RE IMAGINE360, LLC DATA SECURITY INCIDENT LITIGATION	Case No. 23-2603 **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Anthony Collins and Dawn McGee (collectively, "Plaintiffs,") individually and on behalf of all similarly situated persons, allege the following against Imagine360, LLC ("Imagine360" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its multiple failures to properly secure and safeguard their and other similarly situated individuals' (defined herein as "Class Members") personally identifiable information ("PII") and protected health information ("PHI"), including names, addresses, medical billing and insurance information, certain medical information such as diagnoses and medication, and demographic information such as dates of birth and Social Security numbers (the "Private Information"), from unauthorized disclosure to cybercriminals.

2. Defendant Imagine360 is a healthcare revenue cycle company located in Wayne, Pennsylvania that maintains the PII and PHI of patients and/or employees of its clients, including Plaintiffs' employers.

3. Plaintiffs bring this class action lawsuit to address Defendant's collective inadequate safeguarding and supervision of Class Members' Private Information that it collected and maintained, and its failure to adequately supervise its business associates, vendors, and/or suppliers and timely detect the Data Breaches.

4. Imagine360 publicly disclosed that it was impacted by two separate cyberattacks involving its file sharing solutions.[1] The first was detected on or around January 28, 2023 when suspicious activity was discovered within its Citrix file-sharing solution. The second was carried out through a vulnerability exploited in Fortra, LLC's GoAnywhere file-transfer solution. These two separate incidents (collectively referred to herein as the "Data Breaches") impacted different file sharing platforms utilized by Imagine360 during or around the same time period.

5. Threat actors from the ransomware group, "Royal," are suspected to have exploited the Citrix vulnerability,[2] while the Russia-linked ransomware group Clop claimed to be responsible for attacks on GoAnywhere MFT.[3] On February 22, 2023, the U.S. Department of Health and Human Services' ("HHS") Health Sector Cybersecurity Coordination Center issued a "Sector Alert" emphasizing that Clop's claim referenced its ability to target health care systems.

---

[1] *See Imagine360 Suffers Breaches of Two File-Sharing Platforms*, https://www.hipaajournal.com/imagine360-suffers-breaches-of-two-file-sharing-platforms/ (last visited on November 13, 2023).

[2] *See Citrix flaw exploited in ransomware attack against small US business*, https://www.cybersecuritydive.com/news/citrix-vulnerability-exploited-ransomware/640389/ (last visited on November 13, 2023).

[3] *See Imagine360 data breach: medical information, Social Security numbers compromised*, https://cybernews.com/security/imagine360-data-breach/ (last visited on November 13, 2023).

6. In multiple Notice of Security Incident letters (collectively, the "Notice") sent to Plaintiffs and Class Members and state attorneys general, Defendant confirmed that the PII and PHI of certain of its clients' patients and/or employees, including that of Plaintiffs, were exposed by the threat actors in the Data Breaches.

7. Upon information and belief, Defendant knew, prior to January 28, 2023, of the vulnerabilities in its internal file transfer systems and of its business associates' lax data security practices, procedures, and protocols relating to the file-transfer solutions. As such, Defendant could have prevented the Data Breaches. However, Defendant's business associates had to inform Defendant of the Data Breaches *after* the compromise and exfiltration of Plaintiffs' and Class Members' Private Information (by two cybercriminal groups) had already occurred.

8. Defendant also could have prevented this theft had it limited the information it shared with its business associates – particularly Citrix and Fortra – and employed reasonable supervisory measures to ensure that adequate data security practices, procedures, and protocols were being implemented and maintained by within the file-transfer platforms at issue in order to secure and protect the Private Information.

9. Defendant failed to comply with industry standards to protect highly sensitive PII and PHI and failed to provide adequate notice to Plaintiffs and other Class Members that their PII and PHI had been compromised. Plaintiffs seek, among other things, orders requiring Defendant to fully and accurately disclose the nature of the information that has been compromised and to adopt sufficient security practices and safeguards to prevent incidents like the Data Breaches in the future.

10. Plaintiffs and Class Members would not have allowed their Private Information to be entrusted to Defendant if they had known that Defendant would breach its promises and

agreements by failing to use adequate security measures to safeguard it against compromise and exfiltration.

11. Armed with the Private Information accessed in the Data Breaches, the data thieves who carried out the Data Breaches can and will commit a variety of crimes against Plaintiffs and Class Members, including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

12. There has been no assurance offered by Defendant that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices, including the adequate monitoring of its externally hosted file-transfer platforms, sufficient to avoid a similar breach of its network in the future.

13. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, including out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breaches, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breaches.

14. Plaintiffs bring this class action lawsuit to address Defendant's inadequate safeguarding and supervision of Class Members' Private Information that it collected and maintained. The potential for improper disclosure and theft of Plaintiffs' and Class Members'

Private Information was a known risk to Defendant, thus Defendant was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

15. Upon information and belief, Defendant failed to properly supervise its business associates and monitor the platforms that housed the Private Information. Had Defendant provided adequate supervision over its agents, vendors, and/or suppliers, it could have prevented the Data Breaches.

16. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct as the Private Information that Defendant collected and maintained and failed to monitor is now in the hands of data thieves and other unauthorized third parties.

17. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breaches.

II. PARTIES

18. Plaintiff Anthony Collins is, and at all times mentioned herein was, an individual citizen of the State of Illinois.

19. Plaintiff Dawn McGee is, and at all time mentioned herein was, an individual citizen of the Commonwealth of Pennsylvania.

20. Since the Data Breaches, Plaintiffs have noticed a substantial increase in the number of spam emails and spam calls they now receive as compared to the number they received before the Data Breaches occurred. Plaintiffs have further suffered emotional distress, including feelings of fear and anxiety, as a result of their Private Information being accessed and exfiltrated by unauthorized third-party cybercriminals.

21. Defendant Imagine360, LLC is headquartered and maintains its principal place of business at 1550 Liberty Ridge Dr. #330, Wayne, Pennsylvania in Delaware County.

22. Upon information and belief, Imagine360 has two limited liability members– Stephen Kelly and Charles Walters, III.

23. Imagine360 member, Stephen Kelly, is an adult who, at all relevant times, is a resident and citizen of the Commonwealth of Pennsylvania.

24. Imagine360 member, Charles Walters, III, is an adult who, at all relevant times, is a resident and citizen of the State of Georgia.

25. Imagine360 is a citizen of each of the states in which one of its members is a citizen. Imagine360, thus, is a citizen of the Commonwealth of Pennsylvania and the State of Georgia.

26. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs.

27. Plaintiffs will seek leave of court to amend this Complaint to reflect the true names and capacities of such responsible parties when their identities become known.

III. JURISDICTION AND VENUE

28. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Minimal diversity is established because Plaintiff Collins (and many members of the Class) are citizens of states different than Imagine360.

29. This Court has general personal jurisdiction over Imagine360 because Imagine360's principal place of business and headquarters are in this District. Imagine360 also regularly conducts substantial business in this District.

30. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because a substantial part of the events giving rise to the claims emanated from activities within this District, and Imagine360 conducts substantial business in this District.

IV. FACTUAL ALLEGATIONS

A. Defendant's Business and Collection of Plaintiffs' and Class Members' Private Information

31. Imagine360 provides self-funded health insurance plan services to employers within a number of different industries, including auto dealing, convenience stores, construction, manufacturing, nonprofits, marine services, restaurants, senior living, trucking and transportation, technology, and professional services.[4]

32. According to its own website, Imagine360 was founded on the "powerful idea" that "[h]ealth plans can do better[,]" and "[e]mployees should get the high-quality care they need at a fair price."[5]

33. As a condition of receiving these services, Defendant requires that its employer clients, including Plaintiffs' employer, turn over highly sensitive employee personal and health information.

34. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties owed to them and

[4] *See* https://www.imagine360.com/industries/ (last visited on July 6, 2023).

[5] *See* https://www.imagine360.com/about/ (last visited on July 6, 2023).

knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

35. Plaintiffs and Class Members relied on Defendant to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

B. The Data Breaches

36. Fortra and Citrix were Defendant's "business associates." Nevertheless, on or around January 28, 2023, Defendant experienced a breach of its Citrix file-sharing platform that impacted its clients' patients' and/or employees' Private Information, resulting in the compromise and theft thereof by the cybercriminal group, Royal.

37. Soon thereafter, on February 1, 2023, cybersecurity expert Brian Krebs reported that Fortra disclosed to its customers a "remote code injection exploit" affecting GoAnywhere MFT, Fortra's widely used file transfer application. The Russia-linked ransomware group, Clop, used "remote code injection exploits" to remotely execute malicious code on their targets' computer systems and steal data exposed by the software.

38. On or around June 30, 2023 and July 21, 2023, respectively, Imagine360 reported through its Notices to the Maine Attorney General's office and by direct letter notice to Plaintiffs and Class Members that it was impacted by these two Data Breaches, and that the PII and PHI of certain patients and/or employees of its clients, including Plaintiffs' employers, were exposed in the attacks.

39. Through the Data Breaches, the unauthorized cybercriminals accessed a cache of highly sensitive Private Information, including sensitive medical information and health insurance information.

40. Defendant delivered its Notices to Plaintiffs and Class Members several months following the Data Breaches, alerting them that their highly sensitive Private Information had been exposed.

41. Defendant had obligations created by contract, industry standards, common law, federal and state regulations, and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

42. Plaintiffs and Class Members permitted their employers to provide their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such Information confidential and secure from unauthorized access. In Plaintiffs' case, their Private Information was provided to Defendant in order to process claims associated with their health insurance plan obtained through their employer.

43. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

44. Defendant knew or should have known that its electronic records would be targeted by cybercriminals, particularly in light of Citrix's recent history of data breaches.[6]

C. The Healthcare Sector is Particularly Susceptible to Data Breaches

45. Defendant was on notice that companies in the healthcare industry, including its business associate, Citrix, are susceptible targets for data breaches.

46. Defendant was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems,

[6] *See* https://krebsonsecurity.com/2020/02/hackers-were-inside-citrix-for-five-months/; *see also* https://www.cybersecuritydive.com/news/citrix-vulnerability-exploited-ransomware/640389/ (last visited on July 6, 2023).

Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[7]

47. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting confidential medical information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[8]

48. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[9] In 2022, the largest growth in data compromises occurred in the healthcare sector.[10]

49. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident … came to about $20,000," and that the victims

---

[7] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at* https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited on April 28, 2023).

[8] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n. (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited on April 28, 2023).

[9] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/2018-data-breaches/ (last visited on April 28, 2023).

[10] Identity Theft Resource Center, *2022 End-of-Yeare Data Breach Report, available at*: https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited on April 28, 2023).

were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[11]

50. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[12]

51. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[13]

52. Defendant knew, or should have known, the importance of safeguarding its clients' patients' and/or employees' Private Information, including PHI, entrusted to it, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on affected individuals as a result of a data breach.

[11] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited on April 28, 2023).

[12] *Id.*

[13] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited on April 28, 2023).

Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breaches from occurring.

D. Defendant Failed to Comply with HIPAA

53. Title II of HIPAA contains what are known as the Administration Simplification provisions. *See* 42 U.S.C. §§ 1301, *et seq*. These provisions require that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI similar to the data Defendant left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

54. The Data Breaches resulted from a combination of insufficiencies that indicate Defendant failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from the Data Breaches that Defendant either failed to implement, or inadequately implemented, information security policies or procedures to protect Plaintiffs' and Class Members' PHI.

55. Plaintiffs' and Class Members' Private Information compromised in the Data Breaches included "protected health information" as defined by CFR § 160.103.

56. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

57. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

58. Plaintiffs' and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

59. Plaintiffs' and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breaches.

60. Based upon Imagine360's Notice to Plaintiffs and Class Members, Defendant reasonably believes that Plaintiffs' and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breaches.

61. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breaches was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

62. Defendant reasonably believes that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breaches was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

63. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breaches, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

64. Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breaches.

65. Defendant reasonably believes that Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breaches.

66. It is reasonable to infer that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breaches, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

67. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

68. After receiving notice that they were victims of the Data Breaches (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

69. Defendant's security failures also include, but are not limited to:

a. Failing to maintain adequate data security systems, practices, and protocols to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity *or business associate* creates, receives, maintains, or transmits" and "protect against any reasonably anticipated threats or hazards to the security or integrity of such information," in violation of 45 C.F.R. § 164.306 (emphasis added);

d. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

h. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3); and

i. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

70. Because Defendant failed to comply with HIPAA, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is also necessary to ensure Defendant's approach to information security, especially as such approach relates to the supervision of its business associates, vendors, and/or suppliers, is adequate and appropriate going forward. Defendant still maintains the PHI and other highly sensitive PII of its clients' current and

former patients and/or employees. Without the supervision of the Court through injunctive relief, Plaintiffs' and Class Members' Private Information remains at risk of subsequent data breaches.

E. Defendant Failed to Comply with FTC Guidelines

71. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

72. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should ensure the protection of the personal customer information that they collect, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

73. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for

suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

74. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

75. As evidenced by the Data Breaches, Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

76. Defendant was at all times fully aware of its obligations to protect the Private Information of its clients' patients and/or employees yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. Defendant Breached Its Duty to Safeguard Plaintiffs' and Class Members' Private Information

77. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and

protocols (and those of its business associates, vendors, and/or suppliers) adequately protected the Private Information of Class Members.

78. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data (and those of its business associates, vendors, and/or suppliers). Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to adequately protect Class Members' Private Information;

b. Failing to sufficiently train and/or monitor its business associates, vendors, and/or suppliers regarding the proper handling of its clients' patients' and/or employees' Private Information;

c. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

d. Failing to adhere to HIPAA and industry standards for cybersecurity, as discussed above; and

e. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

79. Had Defendant remedied the deficiencies in its information storage and security practices, procedures, and protocols, followed industry guidelines, and adopted data security monitoring, supervision, and other measures recommended by experts in the field, it could have prevented the theft of Plaintiffs' and Class Members' confidential Private Information.

80. Accordingly, Plaintiffs' and Class Members' lives have been severely disrupted. What's more, they have been harmed as a result of the Data Breaches and now face an increased risk of future harm that includes, but is not limited to, medical fraud and identity theft.

G. Defendant Should Have Known that Cybercriminals Target PII and PHI to Carry Out Fraud and Identity Theft

81. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[14] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

82. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

83. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired

[14] *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on April 28, 2023).

information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

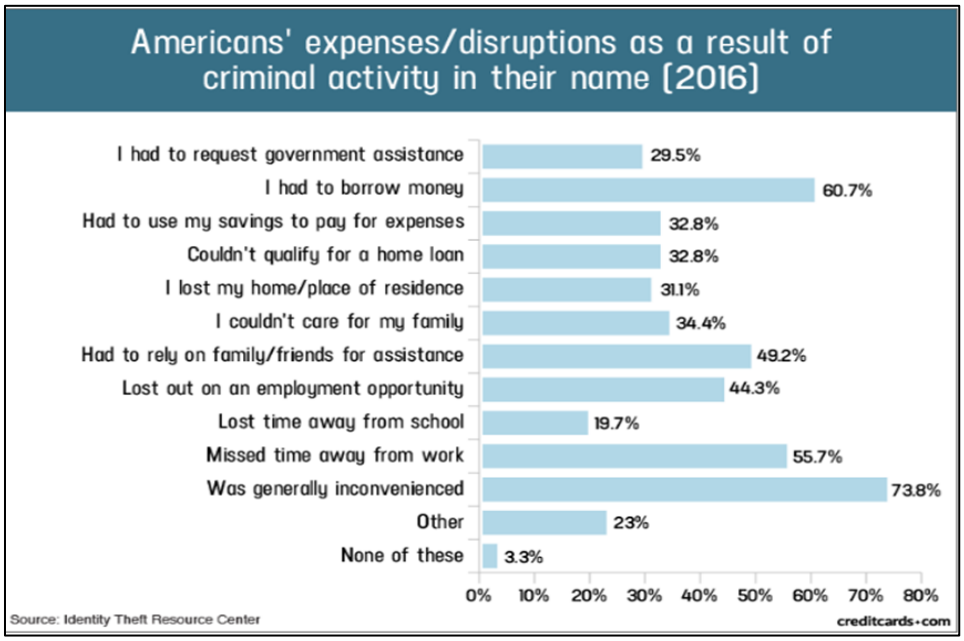
84. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

85. Thus, even if certain information was not purportedly involved in the Data Breaches, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

86. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[15] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

[15] *See IdentityTheft.gov*, Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited April 28, 2023).

87. In fact, a study by the Identity Theft Resource Center[16] shows the multitude of harms caused by fraudulent use of PII:



88. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[17]

89. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

[16] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited on April 28, 2023).

[17] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited on April 28, 2023).

90. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[18]

91. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

92. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[19]

93. The ramifications of Defendant's failure to keep its clients' patients' and/or employees' Private Information secure are long-lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

94. Here, not only was sensitive medical information compromised, but Social Security numbers may have been compromised too. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal

[18] Center for Internet Security, *Data Breaches: In the Healthcare Sector*, *available at*: https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited on April 28, 2023).

[19] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at*: https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited on April 28, 2023).

identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

95. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[20]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

96. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

97. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

H. Plaintiffs' and Class Members' Damages

98. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breaches.

[20] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited April 28, 2023).

99. Plaintiffs and Class Members entrusted their Private Information to Defendant in order to receive Defendant's services. Specifically, Plaintiffs entrusted their Private Information to Defendant when they became an employee of Defendant's clients.

100. Plaintiffs' and Class Members' Private Information was subsequently compromised as a direct and proximate result of the Data Breaches, which Data Breaches resulted from Defendant's inadequate data security practices, procedures, and protocols, as discussed herein.

101. As a direct and proximate result of Defendant's actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, along with other targeted forms of medical identity theft.

102. Further, as a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to spend time dealing with the effects of the Data Breaches. Specifically, Plaintiffs and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and/or closely reviewing and monitoring bank accounts, credit reports, and explanations of benefits for unauthorized activity for years to come.

103. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breaches.

104. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber criminals in the Data Breaches. Numerous courts have

recognized the propriety of loss of value damages in related cases. Indeed, an active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[21] In fact, the data marketplace is so sophisticated that consumers can sell their non-public information directly to a data broker who in turn aggregates the information and provides it to other companies.[22] Consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[23]

105. As a result of the Data Breaches, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

106. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

107. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed

[21] See Data Coup, https://datacoup.com/ (last visited on May 30, 2023).
[22] *What is digi.me?, DIGI.ME,* https://digi.me/what-is-digime/ (last visited on May 30, 2023).
[23] *Frequently Asked Questions,* Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited May 30, 2023).

mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted medical fraud and/or identity theft against them.

108. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breaches in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breaches. These losses include, but are not limited to, the following, monitoring and reviewing explanations of benefits for fraudulent medical charges for years to come, as well as placing "freezes" and "alerts" with credit reporting agencies.

109. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Defendant and its business associates, vendors, and/or suppliers, is protected from future breaches by the implementation of more adequate data security measures and safeguards.

110. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

111. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Fed. R. Civ. P. 23.

112. Specifically, Plaintiffs propose the following Nationwide Class (also referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
> **All individuals in the United States whose Private Information was accessed and/or acquired as a result of one or both of the Data Breaches, including all to whom Defendant sent a data breach notice letter(s).**

113. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which they have a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

114. Plaintiffs reserve the right to modify or amend the definition of the proposed Class or add subclasses before the Court determines whether certification is appropriate.

115. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact identities of Class Members are unknown at this time, based on information and belief, the Class consists of over one hundred thousand individuals whose data was compromised in the Data Breaches. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

116. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct violated the FTCA and/or HIPAA;

c. Whether and to what extent Defendant had an independent, non-delegable duty to protect the Private Information of Class Members;

d. When Defendant learned of the vulnerabilities that led to the Data Breaches;

e. Whether Defendant's response to the Data Breaches was adequate;

f. Whether Defendant took reasonable steps and measures to safeguard Plaintiffs' and Class Members' Private Information;

g. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

h. Whether hackers obtained Class Members' Private Information via the Data Breaches;

i. Whether Defendant knew or should have known that its data monitoring and supervision processes were deficient;

j. Whether Defendant was aware that its business associates', vendors', and/or suppliers' data security practices, procedures, and protocols were inadequate;

k. What damages Plaintiffs and Class Members suffered as a result of Defendant's misconduct;

l. Whether Defendant's conduct was negligent;

m. Whether Defendant were unjustly enriched;

n. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

o. Whether Plaintiffs and Class Members are entitled to lifetime credit or identity monitoring and monetary relief; and

p. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

117. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breaches. Plaintiffs' claims are typical of those of the other Class Members because, *inter*

alia, all Class Members were injured through the common misconduct of Defendant. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

118. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

119. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way and as a result of the same negligent acts and omissions committed by Defendant. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

120. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a class action presents far fewer management

difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

121. Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

122. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class Members affected by the Data Breaches. Class Members have already been preliminarily identified and sent notice of the Data Breaches by Defendant.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

123. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

124. Imagine360 owed a duty under common law to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII and PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

125. Imagine360's duty to use reasonable care arose from several sources, including but not limited to those described below.

126. Imagine360's has a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By receiving, maintaining, and

handling PII and PHI that is routinely targeted by criminals for unauthorized access, Imagine360 was obligated to act with reasonable care to protect against these foreseeable threats.

127. Imagine360's duty also arose from Defendant's position as a business associate of healthcare providers. Imagine360 holds itself out as a trusted provider of health plan solutions, thereby assuming a duty to reasonably protect the information it obtains from its clients. Indeed, Imagine360, who receives, maintains, collects, and handles PII and PHI from the patients and/or employees of its clients, was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breaches.

128. Imagine360 breached the duties owed to Plaintiffs and Class Members and was thus negligent. Although the exact methodologies employed by the unauthorized third parties are unknown to Plaintiffs at this time, on information and belief, Defendant breached its duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Breaches at the time they began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices published to its clients' patients and/or employees; and (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive PII or PHI.

129. But for Imagine360's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their PII and PHI would not have been compromised.

130. As a direct and proximate result of Imagine360's negligence, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breaches – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant

would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class members.

131. As a direct and proximate result of Imagine360's negligence, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

132. Plaintiffs restate and reallege the preceding factual allegations set forth above as if fully alleged herein.

133. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant for failing to use reasonable measures to protect PII and PHI. Various FTC publications and orders also form the basis of Imagine360's duty.

134. Imagine360 violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with the industry standards. Defendant's conduct was

particularly unreasonable given the nature and amount of PII and PHI its obtained and stored and the foreseeable consequences of a data breach involving the PII and PHI its entrusted from its clients' patients and/or employees.

135. Plaintiffs and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

136. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

137. Imagine360 is an entity covered under the HIPAA, which sets minimum federal standards for privacy and security of PHI.

138. Pursuant to HIPAA, 42 U.S.C. §§ 1302d, *et seq.*, and its implementing regulations, Imagine360 had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguards to protect Plaintiffs' and the Class Members' electronic PHI as well as timely notify Plaintiffs' and Class Members of a breach of their PHI.

139. Specifically, HIPAA required Defendant to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR §§ 164.102, *et seq.*

140. Defendant violated HIPAA by actively disclosing Plaintiffs' and the Class Members' electronic PHI; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PHI; and by failing to timely notify Plaintiffs and Class Members of a breach of their PHI.

141. Plaintiffs and the Class Members are patients within the class of persons HIPAA was intended to protect, as they are patients and/or employees of Imagine360's clients.

142. Imagine360's violation of HIPAA constitutes negligence *per se*.

143. The harm that has occurred as a result of Imagine360's conduct is the type of harm that the FTC Act and HIPAA were intended to guard against.

144. As a direct and proximate result of Imagine360's negligence, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their PII and/or PHI;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breaches – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;

g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII and PHI to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class members.

145. As a direct and proximate result of Imagine360's negligence, Plaintiffs and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT III
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

146. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

147. Defendant provided insurance services to Plaintiffs and Class Members through their respective employers. Plaintiffs and Class Members formed an implied contract with Defendant regarding the provision of those services, including by Plaintiffs and Class Members providing their Private Information to Defendant in exchange for the services offered.

148. Through Defendant's offering of services, it knew or should have known that it needed to protect Plaintiffs' and Class Members' confidential Private Information in accordance with Defendant's policies, practices, and applicable state and federal law.

149. As consideration, Plaintiffs and Class Members turned over valuable Private Information to Defendant. Accordingly, Plaintiffs and Class Members bargained with Defendant to securely maintain and store their Private Information.

150. Defendant accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members.

151. In delivering their Private Information to Defendant in exchange for Defendant's services, Plaintiffs and Class Members intended and understood that Defendant would adequately safeguard the Private Information as part of those services.

152. Defendant's implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information, including its business associates, vendors, and/or suppliers, also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its business associates, vendors, and/or suppliers is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees, business associates, vendors, and/or suppliers; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper

encryption; (6) implementing multifactor authentication for access; (7) complying with HIPAA standards to make sure that Plaintiffs' and Class Members' PHI would remain protected; and (8) taking other steps to protect against foreseeable data breaches.

153. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of such an implied contract.

154. Had Defendant disclosed to Plaintiffs and the Class that it did not have adequate data security and data supervisory practices to ensure the security of their sensitive data, Plaintiffs and Class Members would not have provided their Private Information to Defendant.

155. As a provider of health insurance services, Defendant recognized (or should have recognized) that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiffs and the Class.

156. Defendant violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information. Defendant further breached these implied contracts by failing to comply with its promise to abide by HIPAA.

157. Additionally, Defendant breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information they created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

158. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

159. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

160. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2).

161. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

162. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations, in violation of 45 CFR 164.306(a)(94).

163. Defendant further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq*.

164. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in violation of 45 CFR 164.530(c).

165. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality, integrity, and availability of all electronic

protected health information its business associate(s) "create, receive, maintain, or transmit" and "protect against any reasonably anticipated threats or hazards to the security or integrity of such information," in violation of 45 C.F.R. § 164.306 (emphasis added).

166. Defendant further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PHI.

167. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide accurate and complete Private Information and to pay Defendant in exchange for Defendant's agreement to, *inter alia*, protect their Private Information.

168. Plaintiffs and Class Members have been damaged by Defendant's conduct, including the harms and injuries arising from the Data Breaches now and in the future, as alleged herein.

COUNT IV
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

169. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

170. This Count is pleaded in the alternative to Count II above.

171. Upon information and belief, Defendant entered into virtually identical contracts with its clients, including Plaintiffs' employers and/or healthcare providers, to provide health plan services to them. These services included material terms regarding Defendant's implementation of data security practices, procedures, and protocols sufficient to safeguard the Private Information that was to be entrusted to it.

172. Such contracts were made expressly for the benefit of Plaintiffs and the Class, as it was their Private Information that Defendant agreed to receive and protect through its services.

Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties and Plaintiffs and Class Members were direct and express beneficiaries of such contracts.

173. Defendant knew that if it were to breach these contracts with its clients, Plaintiffs and the Class, would be harmed.

174. Defendant breached its contracts with its clients and, as a result, Plaintiffs and Class Members were affected by these Data Breaches when Defendant failed to use reasonable data security and/or business associate monitoring measures that could have prevented the Data Breaches.

175. As foreseen, Plaintiffs and the Class were harmed by Defendant's failure to use reasonable data security measures to securely store and protect the files in its care, including but not limited to, the continuous and substantial risk of harm through the loss of their Private Information.

176. Accordingly, Plaintiffs and the Class are entitled to damages in an amount to be determined at trial, along with costs and attorneys' fees incurred in this action.

COUNT V
UNJUST ENRICHMENT/QUASI CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

177. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

178. This Count is pleaded in the alternative to Counts II and III above.

179. Plaintiffs and Class Members conferred a benefit on Defendant. Specifically, they provided Defendant with their Private Information, which Private Information has inherent value. In exchange, Plaintiffs and Class Members should have been entitled to Defendant's adequate

protection and supervision of their Private Information, especially in light of their special relationship.

180. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiffs' retained data and used Plaintiffs' and Class Members' Private Information for business purposes.

181. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their Private Information provided.

182. Defendant acquired the Private Information through inequitable record retention as it failed to disclose the inadequate data security practices previously alleged.

183. If Plaintiffs and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would have required that alternative choices be made by their respective employers that excluded Defendant.

184. Plaintiffs and Class Members have no adequate remedy at law.

185. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

186. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) the imminent and substantial risk of actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity

theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breaches, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breaches for the remainder of the lives of Plaintiffs and Class Members.

187. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

188. Plaintiffs and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VI
BREACH OF CONFIDENCE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

189. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

190. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by Defendant and ultimately accessed and acquired in the Data Breaches.

191. As a provider of employer health plans, Defendant has a special relationship with the patients and/or employees of its clients, including Plaintiffs and Class Members. Because of that special relationship, Defendant was provided with and stored Plaintiffs' and Class Members' Private Information and had a duty to ensure that such was maintained in confidence.

192. Individuals like Plaintiffs and Class Members have a privacy interest in personal, medical and other matters, and Defendant had a duty not to permit the disclosure of such matters concerning Plaintiffs and Class Members.

193. As a result of the parties' special relationship, Defendant had possession and knowledge of highly sensitive and confidential PHI and PII belonging to Plaintiffs and Class Members, information that was not generally known.

194. Plaintiffs and Class Members did not consent nor authorize Defendant to release or disclose their Private Information to an unknown criminal actor.

195. Defendant breached its duty of confidence owed to Plaintiffs and Class Members by, among other things: (a) failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of employee member information that resulted in the unauthorized access and compromise of Plaintiffs' and Class Members' Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards (and those of its business associates, vendors, and/or suppliers) in place to control these risks; (c) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (d) failing to follow its own privacy policies and practices published to clients and their patients and/or

employees; and (e) making an unauthorized and unjustified disclosure and release of Plaintiffs' and Class Members' Private Information to a criminal third party.

196. But for Defendant's wrongful breach of its duty of confidence owed to Plaintiffs and Class Members, their Private Information would not have been compromised.

197. As a direct and proximate result of Defendant's wrongful breach of its duty of confidence, Plaintiffs and Class Members have suffered and will continue to suffer the injuries alleged herein.

198. It would be inequitable for Defendant to retain the benefit of controlling and maintaining Plaintiffs' and Class Members' Private Information at the expense of Plaintiffs and Class Members.

199. Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT VII
INJUNCTIVE/DECLARATORY RELIEF
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

200. Plaintiffs restate and reallege the allegations in the preceding paragraphs as if fully set forth herein.

201. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state statutes described in this Complaint.

202. Defendant owes a duty of care to Plaintiffs and Class Members, which required them to adequately monitor and safeguard Plaintiffs' and Class Members' Private Information.

203. Defendant and its associates, vendors, and/or suppliers still possess the Private Information belonging to Plaintiffs and Class Members.

204. Plaintiffs allege that Defendant's data security measures remain inadequate. Furthermore, Plaintiffs continues to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

205. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure its clients' patients' and/or employees' Private Information under the common law, HIPAA, and the FTCA;

b. Defendant's existing data monitoring measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable data security procedures and practices that are appropriate to protect Private Information; and

c. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure its clients' patients' and/or employees' Private Information.

206. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with legal and industry standards to protect the highly sensitive Private Information that remains in its possession and control, including the following:

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security and monitoring measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its clients and its clients' patients and/or employees about the threats they face with regard to the security of their Private Information, as well as the steps that should be taken to protect themselves.

207. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach similar to the Data Breaches giving rise to this Action. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

208. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

209. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach similar to the Data Breaches that are the subject of this Complaint, thus preventing future injury to Plaintiffs and other individuals whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seeks the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;

b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Defendant to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring Defendant to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: November 13, 2023 Respectfully submitted,

/s/ Nicholas Sandercock

Nicholas Sandercock
Mason A. Barney (*pro hac vice* to be filed)
Tyler J. Bean (*pro hac vice* to be filed)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: nsandercock@sirillp.com
E: mbarney@sirillp.com
E: tbean@sirillp.com

Gary F. Lynch
Jamisen A. Etzel
Nicholas A. Colella
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
gary@lcllp.com
jamisen@lcllp.com
nickc@lcllp.com

Attorneys for Plaintiffs